CLAIMS

1. A method of remotely controlling a security element of a mobile terminal for disabling and enabling access to secured functions of the mobile terminal, the method comprising:

receiving a request from a user;

verifying authenticity of the user;

creating a signed push message including, at least, an address for the mobile terminal and content which causes a disablement application to be executed; and

sending the signed push message to the mobile terminal.

2. The method of claim 1 wherein the request and the push message are for disabling access, and further comprising:

receiving a confirmation message from the mobile terminal; and

sending a response message to the user based on the confirmation message.

3. The method of claim 1 wherein the request from the user and the push message are for disabling access, and further comprising:

determining that the mobile terminal is unavailable; and

sending a response message to the user based on a determination that the mobile terminal is unavailable.

4. The method of claim 2 wherein the confirmation message from the mobile terminal is signed.

5. The method of claim 4 wherein the confirmation message and the response include position information for the mobile terminal.

6. The method of claim 1 wherein the request and the push message are for enabling access, and further comprising:

receiving a confirmation message from the mobile terminal; and

sending a response message to the user based on the confirmation message.

7. The method of claim 1 wherein the content comprises an identification of an application that resides in the mobile terminal.

8. The method of claim 1 wherein the content comprises an identification of a calling program residing at a server.

9. The method of claim 2 wherein the content comprises an identification of an application that resides in the mobile terminal.

10. The method of claim 2 wherein the content comprises an identification of a calling program residing at a server.

11. The method of claim 3 wherein the content comprises an identification of an application that resides in the mobile terminal.

12. The method of claim 3 wherein the content comprises an identification of a calling program residing at a server.

13. The method of claim 4 wherein the content comprises an identification of an application that resides in the mobile terminal.

14. The method of claim 4 wherein the content comprises an identification of a calling program residing at a server.

15. The method of claim 5 wherein the content comprises an identification of an application that resides in the mobile terminal.

16. The method of claim 5 wherein the content comprises an identification of a calling program residing at a server.

17. The method of claim 6 wherein the content comprises an identification of an application that resides in the mobile terminal.

18. The method of claim 6 wherein the content comprises an identification of a calling program residing at a server.

19. Apparatus for remotely controlling a security element of a mobile terminal for disabling and enabling access to functions of the mobile terminal, the apparatus comprising:

means for receiving a request from a user;

means for verifying authenticity of the user;

means for creating a signed push message including, at least, an address for the mobile terminal and content which causes a disablement application to be executed;

means for sending the signed push message to the mobile terminal;

Doc 1 of 1 - 0 - 0 - 0

means for receiving a confirmation message from the mobile terminal; and

means for sending a response to the user based the confirmation message.

20. A computer program product for enabling a computer system to remotely control a security element of a mobile terminal for disabling and enabling access to secured functions of the mobile terminal, the computer program product including a computer program comprising:

instructions for receiving a request from a user;

instructions for verifying authenticity of the user;

instructions for creating a signed push message including, at least, an address for the mobile terminal and content which causes a disablement application to be executed;

instructions for sending the signed push message to the mobile terminal; and

instructions for sending a response to the user based on an outcome of the sending of the signed push message.

21. The computer program product of claim 20 wherein the content comprises an identification of an application that resides in the mobile terminal.

22. The computer program product of claim 20 wherein the content comprises an identification of a calling program residing at a server.

23. The computer program product of claim 20 further comprising:

instructions for receiving position information for the mobile terminal within a signed confirmation message from the mobile terminal when the request and the signed push message are for disabling access; and

instructions for including the position information for the mobile terminal in the response.

24. The computer program product of claim 21 further comprising:

instructions for receiving position information for the mobile terminal within a signed confirmation message from the mobile terminal when the request and the signed push message are for disabling access; and

instructions for including the position information for the mobile terminal in the response.

25. The computer program product of claim 22 further comprising:

instructions for receiving position information for the mobile terminal within a signed confirmation message from the mobile terminal when the request and the signed push message are for disabling access; and

instructions for including the position information for the mobile terminal in the response.

26. A programmed computer system operable for controlling a security element of a mobile terminal for disabling and enabling access to secured functions of the mobile terminal by performing a method comprising:

receiving a request from a user;

verifying authenticity of the user;

creating a signed push message including, at least, an address for the mobile terminal and content which causes a disablement application to be executed;

sending the signed push message to the mobile terminal; and

sending a response to the user based on an outcome of the sending of the signed push message.

27. The computer system of claim 26 wherein the content comprises an identification of an application that resides in the mobile terminal.

28. The computer system of claim 26 wherein the content comprises an identification of a calling program residing at a server.

29. The computer system of claim 26 further enabled to:

receive position information for the mobile terminal within a signed confirmation message from the mobile terminal when the request and the signed push message are for disabling access; and

include the position information for the mobile terminal in the response.

30. The computer system of claim 27 further enabled to:

receive position information for the mobile terminal within a signed confirmation message from the mobile terminal when the request and the signed push message are for disabling access; and

include the position information for the mobile terminal in the response.

31. The computer system of claim 28 further enabled to:

receive position information for the mobile terminal within a signed confirmation message from the mobile terminal when the request and the signed push message are for disabling access; and

include the position information for the mobile terminal in the response.

32. A system for controlling a security element of a mobile terminal for disabling and enabling access to secured functions of the mobile terminal, the system comprising:

a push initiator operable to create and send signed push messages including, at least, an address for the mobile terminal and content which causes a disablement application to be executed;

a proxy gateway operable to receive the signed push messages and send over-the-air messages to the mobile terminal corresponding to the signed push messages; and

a network interconnecting the push initiator and the proxy gateway.

33. A mobile terminal comprising:

a radio block;

a security element encoded with at least one security key for securing transactions; and

a processor system operably connected to the radio block and the security element, the processor system further operable to disable and enable access to the key in response to unsolicited, over-the-air messages received through the radio block.

34. The mobile terminal of claim 33 wherein the processor system is further operable to disable access to the at least one security key while permitting operations of the security element for which user authentication and authorization services are not required.

35. The mobile terminal of claim 33 wherein the processor system disables access to the at least one security key by disabling access to the security element.

36. The mobile terminal of claim 34 wherein the security element further comprises at least one status register associated with the at least one security key, and wherein the processor system enables and disables access to the key by alternatively setting the status register to a first state wherein access to the at least one security key is enabled and a second state wherein access to the at least one security key is disabled, respectively.

37. The mobile terminal of claim 33 further comprising a global positioning system (GPS) subsystem, and wherein the processor system is further enabled to cause the mobile terminal to send a confirmation message through the radio block, the confirmation message including position information for the mobile terminal, the position information being retrieved from the GPS subsystem.

38. The mobile terminal of claim 34 further comprising a global positioning system (GPS) subsystem, and wherein the processor system is further enabled to cause the mobile terminal to send a confirmation message through the radio block, the confirmation message including position information for the mobile terminal, the position information being retrieved from the GPS subsystem.

39. The mobile terminal of claim 36 further comprising a global positioning system (GPS) subsystem, wherein the processor system is further enabled to cause the mobile terminal to send a confirmation message through the radio block, the confirmation message including position information for the mobile terminal, the position information being retrieved from the GPS subsystem.

40. A security element for a mobile terminal, the security element encoded with a data structure for providing user authentication services, the data structure comprising:

at least one key for securing at least some transactions initiated by a user of the mobile terminal; and

at least one status indicator associated with the at least one key, the status indicator settable by the mobile terminal alternatively to a first state wherein access to the at least one key is enabled and a second state wherein access to the at least one key is disabled.

41. The security element of claim 40 wherein the at least one key is a plurality of key pairs providing user authentication and authorization services through the use of digital signatures, and wherein the at least one status indicator is a plurality of status indicators, further wherein each status indicator is associated with one key pair.

42. In a mobile terminal, a method of controlling access to a security key in a security element, the method comprising:

receiving an unsolicited, over-the-air request to disable access to the security key in the security element;

updating a status register in the security element to disable access to the security key; and

sending an over-the-air, secured confirmation message indicating success of disabling access to the security key.

43. The method of claim 42 further comprising:

receiving an unsolicited, over-the-air request to re-enable access to the security key in the security element; and

updating a status register in the security element to re-enable access to the security key.

44. The method of claim 42 wherein the unsolicited over-the-air, request to disable access takes the form of a wireless application protocol (WAP) push message.

45. The method of claim 43 wherein the unsolicited over-the-air, request to disable access and the unsolicited, over-the-air request to disable access take the form of a wireless application protocol (WAP) push messages.

46. A mobile terminal comprising apparatus for controlling access to at least one security key in a security element, the apparatus comprising:

means for receiving unsolicited, over-the-air requests to disable access to the at least one security key in the security element and to re-enable access to the at least one security key in the security element;

means for updating a status register in the security element in accordance with requests to disable and re-enable access to the at least one security key; and

means for sending over-the-air, secured confirmation messages indicating success of disabling and re-enabling access to the at least one security key.

47. A mobile terminal comprising:

a radio block;

an interface operable to access a security element encoded with at least one security key; and

a processor system operably connected to the radio block and the security element, the processor system further operable to disable and enable

access to the key in response to unsolicited, over-the-air messages received through the radio block.

48. The mobile terminal of claim 47 wherein the processor system is further operable to disable access to the at least one security key while permitting operations of the security element for which user authentication and authorization services are not required.

49. The mobile terminal of claim 47 wherein the processor system disables access to the at least one security key by disabling access to the security element.

50. The mobile terminal of claim 47 further comprising a global positioning system (GPS) subsystem, and wherein the processor system is further enabled to cause the mobile terminal to send a confirmation message through the radio block, the confirmation message including position information for the mobile terminal, the position information being retrieved from the GPS subsystem.

51. The mobile terminal of claim 48 further comprising a global positioning system (GPS) subsystem, and wherein the processor system is further enabled to cause the mobile terminal to send a confirmation message through the radio block,

the confirmation message including position information for the mobile terminal, the position information being retrieved from the GPS subsystem.